CLASS SPECIFICATION

TITLE	GRADE	EEO-4	CODE
CHIEF INFORMATION SECURITY OFFICER	**44**	**A**	**7.936**
INFORMATION SECURITY OFFICER III	**43**	**B**	**7.937**
INFORMATION SECURITY OFFICER II	**41**	**B**	**7.938**
INFORMATION SECURITY OFFICER I	**39**	**B**	**7.939**

SERIES DISCUSSION

Information Security Officers (ISOs) manage, organize, lead or direct the activities of one or more of the following ten security domain areas within a department, division, unit, program or project:

- access control – centralized / decentralized / remote / federated
- application/system development security – validation / verification / guidelines
- continuity of operations/disaster recovery planning – business recovery
- cryptography – transport / storage / authentication / non-repudiation
- information security management – awareness / policies / risk management / procedural standards
- operational security (OPSEC) – threats / hostile code / techniques
- physical technical security – access systems / structural / environmental controls
- security architecture and models – methods / security operational standards
- security law, investigation and ethics – cyber crime / incident response / security regulation
- telecommunications/network security – enclave / monitoring / vpn / firewall / prevention

****

SERIES CONCEPT

Information Security Officers work on security administration, security operation and/or security oversight for the information systems and data within the assigned area of information security responsibility. Incumbents work with management and technical staff to develop a comprehensive information security program for integrated IT systems within the enterprise or agency.

Develop an organizational information security program in accordance with State security enterprise-wide policies, standards, and procedures; mitigate, accept, and/or avoid vulnerabilities to empower the agency to achieve technical/business goals and objectives; conduct ongoing assessments of the effectiveness of information security activities and technology resources to ensure that the agency has addressed information security appropriately within identified goals, objectives, desired deliverables, and the scope of IT systems being requested, maintained or developed.

Participate in cost and budget estimates for development, hardware and software, and ongoing operating costs for information security expenses; analyze information security requirements for IT projects in terms of development, hardware, software, and personnel requirements.

Develop, present and justify enterprise-wide or agency information security budgets for review and approval and testify before Executive and Legislative groups as required.

Train, supervise and evaluate the performance of lower level staff; provide technical expertise, on an ongoing or project basis, to information security professionals at comparable and lower levels.

Participate in vendor evaluations and contract negotiations; provide contract administration guidance on information security requirements.

SERIES CONCEPT (cont'd)

Establish, implement, and monitor information security policies, procedures and standards for the assigned area of information security responsibility.

Participate in the State security enterprise-wide process.

Participate in State enterprise-wide IT activities and policy-making activities and/or serve on various ad hoc committees and work groups.

Perform related duties as assigned.

****

CLASS CONCEPTS

Chief Information Security Officer: Under administrative direction, incumbents have enterprise-wide or multi-agency information security responsibilities (multi-agency organizations are those agencies excluded from Department of Information Technology oversight pursuant to NRS 242.111). All Chief Information Security Officer (CISO) positions interact with internal and external management levels as well as executives and officials to negotiate solutions to major or controversial security issues. Positions at this level must supervise Information Security Officer III's or multiple information security professionals at comparable and lower levels, on a regular and recurring basis. This class is reserved for the highest level of information security manager in a branch of State government and those organizations excluded from DOIT oversight. Incumbents report to:

1) the Nevada State Chief Information Officer (CIO) and is responsible for the enterprise-wide information security program. The incumbent provides co-leadership to the State Security Committee in planning, developing and implementing information security initiatives at the statewide level within the following functional core components: disaster recovery; technical security administration; accreditation; and assessment/awareness; or

2) the department director or executive of an agency which is excluded from Department of Information Technology oversight as established in NRS 242.111 with responsibility for directing and managing the agency's information security program and providing co-leadership to the State Security Committee or comparable organization providing oversight, planning, and implementation assistance for information security initiatives at the statewide/enterprise/multi-agency level.

Example of a Chief Information Security Officer position:

In the Department of Information Technology, the incumbent oversees State enterprise-wide policies, standards, procedures, and guidelines for information security as developed by the State Security Committee. The incumbent also chairs the State Security Committee and builds consensus with other agency information security professionals throughout the State and local government. The incumbent supervises subordinate Information Security Officers who provide information security services to over 100 State agencies in core functional areas of disaster recovery, technical security administration, accreditation, and assessment/awareness.

This position interacts with local government jurisdictions on a regular basis to implement statewide security programs. In addition, the CISO is accountable for developing and executing information security strategies to meet the evolving business needs of the State, which includes quantifying and prioritizing security enhancement and development requests. This position ensures the security architecture is reliable

CLASS CONCEPTS (cont'd)

Chief Information Security Officer (cont'd)

Example of a Chief Information Security Officer position (cont'd)
and capable of supporting the operational needs of the State and also serves as the department's public information officer, represents the department on the Attorney General's Cyber Crimes Advisory Board, participates with national information security organizations in cooperative efforts, and works with the Department of Public Safety personnel regarding cyber-terrorism with respect to Homeland Security efforts.

Information Security Officer III: Under general direction, incumbents interact with internal and external management levels as well as executives and officials to solve security problems involving conflict or controversy requiring interpretation/application of information security policy. Positions at this level are wholly dedicated to information security and are responsible and accountable for adherence to security policies established by the State Security Committee. The ISO III is distinguished from the II level by the broader scope of responsibility for information security for a major State department or multiple departments. Incumbents report to:

1) the Chief Information Security Officer (CISO) within the Department of Information Technology and are responsible and accountable for adherence to the State security policies; directing and managing the departmental information security program; and serving as the department's representative on the State Security Committee. The incumbent has direct authority for the design, establishment, administration and execution of the department's information security program as well as planning and implementation of information security initiatives at the department level; or

2) the department director, administrator or authorized agency CISO, or agency information technology manager of a major State department. Incumbents are responsible and accountable for adherence to the State security policies and must serve as the department's representative on the State Security Committee. They plan, organize, coordinate and manage the department's information security program to include the design, establishment, administration and implementation of information security initiatives, systems, programs, and activities at the department level.

Example of an Information Security Officer III position:

Within the Office of Information Security in the Department of Information Technology, the incumbent oversees the departmental information security program that consists of departmental computing infrastructures; oversees departmental security service offerings to customer agencies (e.g., mainframe, servers, wide area network, analog/digital microwave transport communication systems) as well as some enterprise-wide computing and communications infrastructure. This position is responsible for the daily direction and management of the Office of Information Security and trains, supervises and evaluates the performance of multiple Information Security Officers.

Information Security Officer II: Under general direction of a department director, division administrator, agency CISO, agency information technology manager, or ISO III, incumbents are responsible for directing and managing the division/unit information security program with direct authority for the design, establishment, administration and execution of a portion of the department/division/unit information security program.

Incumbents perform all or some of the duties described in the series concept at the division/unit level with at least 70% of their daily activities devoted solely to information security. Incumbents interact with internal

CLASS CONCEPTS (cont'd)

Information Security Officer II (cont'd)
and external peers and higher supervisory levels in order to answer questions requiring explanation or interpretation of information security standard procedures, and to solve security problems involving some conflict and requiring interpretation/application of policy. This level is distinguished from the ISO I by the broader scope of responsibility for information security at the division/work unit level.

Example of an Information Security Officer II position:

In the Department of Information Technology, the incumbent in the disaster recovery unit within the Office of Information Security directs and oversees the enterprise-wide Critical Application Disaster Recovery Program with direct authority for enterprise-wide program implementation. This position develops policies, standards, procedures, and guidelines for disaster recovery and continuity of operations in State government; investigates areas for cost effective integration of disaster recovery services with other State agencies and local governments; and prepares and maintains a master plan for the orderly and cost-effective implementation of the State's technical disaster recovery plan. In addition, the incumbent is responsible for evaluation of vendor proposals on disaster recovery services, and participates with technical operations staff to negotiate contractual terms and conditions, and for the implementation, administration and support of the State Critical Application Disaster Recovery Plan which is an intricate and critical part of the State's continuity of government. In addition, the incumbent serves as lead for other disaster recovery unit personnel.

Information Security Officer I: Under limited supervision of a department director, division administrator, agency CISO, agency information technology manager, or ISO III, incumbents perform and implement program/project information security tasks with responsibility for the design, establishment, administration and execution of the assigned portion of the department/division/unit information security program; and for the planning and implementation of information security initiatives at the functional, project or program level. Incumbents perform some or all of the duties described in the series concept at a program/project level with at least 70% of their daily activities devoted solely to information security. Incumbents interact with internal and external peers and supervisory levels in order to answer questions requiring explanations or interpretations of information security standard procedures and to solve security problems involving some conflict and requiring interpretation/application of policy.

Example of an Information Security Officer I position:

In the Department of Information Technology, the incumbent works in the Office of Information Security and maintains the department and enterprise-wide Information Security Assessment Program. The incumbent works with the team lead of the assessment unit to coordinate and conduct security assessments of State agencies; creates and maintains policies, standards, procedures, and guidelines for State and local government; investigates areas of risk within systems and the technical environment; and provides assistance to other State agencies and local governments on security related topics. In addition, the incumbent evaluates vendor proposals on security assessment tools and services, and participates with technical operations staff to identify additional needs for information security programs.

****

MINIMUM QUALIFICATIONS

SPECIAL NOTES AND REQUIREMENTS FOR ALL POSITIONS IN THE SERIES:

Professional certification from a nationally recognized/accredited organization may be substituted for the required experience as follows:

CHIEF INFORMATION SECURITY OFFICER	**44**	**A**	**7.936**
INFORMATION SECURITY OFFICER III	**43**	**B**	**7.937**
INFORMATION SECURITY OFFICER II	**41**	**B**	**7.938**
INFORMATION SECURITY OFFICER I	**39**	**B**	**7.939**

MINIMUM QUALIFICATIONS (cont'd)

SPECIAL NOTES AND REQUIREMENTS (cont'd)

- International Information Systems Security Certification Consortium, Inc (ISC^2) - Certified Information System Security Professional (CISSP) is equivalent to three years of experience.
- Information Systems Audit and Control Association (ISACA) - Certified Information Security Manager (CISM) is equivalent to two years of experience.
- Global Information Assurance Certification (GIAC) - Security Expert is equivalent to two years of experience.
- Other nationally recognized information security certifications may be substituted for up to one year of experience.
- Nevada Information Security Professional (NISP) certification must be obtained within 12 months of appointment and maintained as a condition of employment for Information Security Officers III, II and I (possession of a valid and current CISSP certification meets this requirement).
- CISSP and CISM certification is required at the time of appointment and must be maintained as a condition of employment for the Chief Information Security Officer level.
- Applicants must pass a background investigation as designated by the agency in order to be considered for employment.
- Some positions require specialized knowledge of specific domains and will be identified at the time of recruitment.

CHIEF INFORMATION SECURITY OFFICER

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university in information security, management information systems, computer science or other closely related field plus eight years of professional information security work experience in eight or more information security domains identified in the series discussion section, four years of which must have been in a managerial or supervisory capacity in a large information security/systems environment; **OR** graduation from high school or equivalent education plus ten years of professional information security work experience in eight information security domains identified in the series discussion, four years of which must have been in a managerial or supervisory capacity in a large information security/systems environment; **OR** one year of experience as an Information Security Officer III in Nevada State service; **OR** an equivalent combination of education and experience. *(See Special Notes and Requirements)*

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application):
Detailed knowledge of: eight of the ten information security domains; enterprise-wide regulations, standards, policies and procedures related to information security; strategic planning and project management at the enterprise-wide level. **Ability to:** oversee the development of State enterprise-wide regulations, policies, standards and guidelines; testify before Executive Branch and Legislative groups regarding statewide information security challenges and programs; analyze data, solve problems and make appropriate decisions within eight of the ten domains; plan, organize and manage the functional core components for information security including disaster prevention/recovery, assessment and awareness, technical security administration and accreditation; *and all knowledge, skills and abilities required at the lower levels.*

FULL PERFORMANCE KNOWLEDGE, SKILLS AND ABILITIES (typically acquired on the job):
Working knowledge of: Nevada Revised Statutes pertaining to information systems, services and security. **Ability to:** draft and review Bill Draft Requests.

CHIEF INFORMATION SECURITY OFFICER	**44**	**A**	**7.936**
INFORMATION SECURITY OFFICER III	**43**	**B**	**7.937**
INFORMATION SECURITY OFFICER II	**41**	**B**	**7.938**
INFORMATION SECURITY OFFICER I	**39**	**B**	**7.939**

MINIMUM QUALIFICATIONS (cont'd)

INFORMATION SECURITY OFFICER III

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university in information security, management information systems, computer science or other closely related field plus seven years of professional information security work experience in seven or more information security domains identified in the series discussion, three years of which must have been in a supervisory or project leader capacity in an information security/systems environment; **OR** graduation from high school or equivalent education and nine years of professional information security work experience in seven or more information security domains identified in the series discussion, three years of which must have been in a supervisory or project leader capacity in an information security/systems environment; **OR** two years of experience as an Information Security Officer II in Nevada State service; **OR** an equivalent combination of education and experience. *(See Special Notes and Requirements)*

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application):
Detailed knowledge of: strategic planning and project management at the department level; current information security trends and technology; current principles, theories, practices and procedures of information security management; methods and techniques used to safeguard against accidental or unauthorized modification, destruction or disclosure of data to meet security needs. **Working knowledge of:** seven of the ten security domains; training and supervisory techniques, business practices and principles common to a large, complex organization. **Ability to:** select the best course of mitigation actions for security issues with respect to public and private sector information; analyze data, solve problems, make appropriate decisions, and assess costs and present alternatives within seven of the ten domains; *and all knowledge, skills and abilities required at the lower levels.*

FULL PERFORMANCE KNOWLEDGE, SKILLS AND ABILITIES (typically acquired on the job):
Working knowledge of: Nevada Revised Statutes pertaining to information systems, services and security; State personnel regulations and processes. **Ability to:** testify before Executive Branch and Legislative groups regarding information security programs.

INFORMATION SECURITY OFFICER II

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university in information security, management information systems, computer science or other closely related field plus five years of professional information security work experience in five or more information security domains identified in the series discussion, one year of which must have been in a supervisory or project leader capacity in an information security/systems environment; **OR** graduation from high school or equivalent education plus seven years of professional information security work experience in five or more information security domains identified in the series discussion, one year of which must have been in a supervisory or project leader capacity in an information security/systems environment; **OR** two years of experience as an Information Security Officer I in Nevada State service; **OR** an equivalent combination of education and experience. *(See Special Notes and Requirements)*

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application):
Working knowledge of: current principles, theories, practices and procedures related to information security management; five of the ten information security domains; general-purpose security controls; current information security trends and technologies; strategic planning and project management at the division/work unit level; policy development and implementation; methods and techniques used to safeguard against accidental or unauthorized modification, destruction or disclosure of data to meet security needs; interagency business practices and principles. **Ability to:** identify complex information security risks, vulnerabilities and problems; select the best course of mitigation actions for security issues; assess the security and/or vulnerability of information assets to assist in developing a risk assessment of

MINIMUM QUALIFICATIONS (cont'd)

INFORMATION SECURITY OFFICER II (cont'd)

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application): (cont'd) multiple security domains; assess costs and present alternatives for the assigned area of responsibility; analyze data, solve problems and make appropriate decisions within five of the ten domains; design appropriate solutions to complex security problems; *and all knowledge, skills and abilities required at the lower level.*

FULL PERFORMANCE KNOWLEDGE, SKILLS AND ABILITIES (typically acquired on the job): **Working knowledge of:** departmental regulations, policies, standards and procedures related to IT systems, services and security. **General knowledge of:** State personnel and purchasing regulations.

INFORMATION SECURITY OFFICER I

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university in information security, management information systems, computer science or other closely related field plus three years of professional information security work experience in three or more information security domains identified in the series discussion; **OR** graduation from high school or equivalent education, plus five years of professional information security work experience within three or more information security domains identified in the series discussion; **OR** an equivalent combination of education and experience. *(See Special Notes and Requirements)*

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application): **Working knowledge of:** three of the ten security domains; current principles, theories, practices and procedures of information security management. **General knowledge of:** general-purpose security controls; current information security trends and technologies. **Ability to:** develop plans to safeguard against accidental or unauthorized modification, destruction or disclosure of data to meet security needs; assess costs and present alternatives for the assigned area of responsibility; participate in long-term projects and strategic planning; organize resources and materials in order to meet project timelines; assess the security and/or vulnerability of information assets to assist in developing a risk assessment; analyze data, solve problems and make appropriate decisions within three of the ten domains; provide effective and responsive customer service; establish and maintain positive working relationships with others; develop and implement information security training materials and workshops. **Skilled in:** technical writing, report preparation and oral communication.

FULL PERFORMANCE KNOWLEDGE, SKILLS AND ABILITIES (typically acquired on the job): **Working knowledge of:** State enterprise-wide and department regulations, policies, standards, and procedures; Nevada Revised Statutes pertaining to information systems, services and security. **General knowledge of:** State Personnel regulations and processes. **Ability to:** identify information security risks, vulnerabilities and problems for an agency. **Skilled in:** agency business principles, practices and activities.

CHIEF INFORMATION SECURITY OFFICER	**44**	**A**	**7.936**
INFORMATION SECURITY OFFICER III	**43**	**B**	**7.937**
INFORMATION SECURITY OFFICER II	**41**	**B**	**7.938**
INFORMATION SECURITY OFFICER I	**39**	**B**	**7.939**

This class specification is used for classification, recruitment and examination purposes. It is not to be considered a substitute for work performance standards for positions assigned to this series.

	7.936	7.937	7.938	7.939
ESTABLISHED:	7/1/05R 9/23/05PC	7/1/05R 9/23/05PC	7/1/05R 9/23/05PC	7/1/05R 9/23/05PC